The Implementation of Homeland Security Presidential Directive 12

David Temoshok
Director, Identity Policy and Management
GSA Office of Governmentwide Policy

GSA Industry Day 2
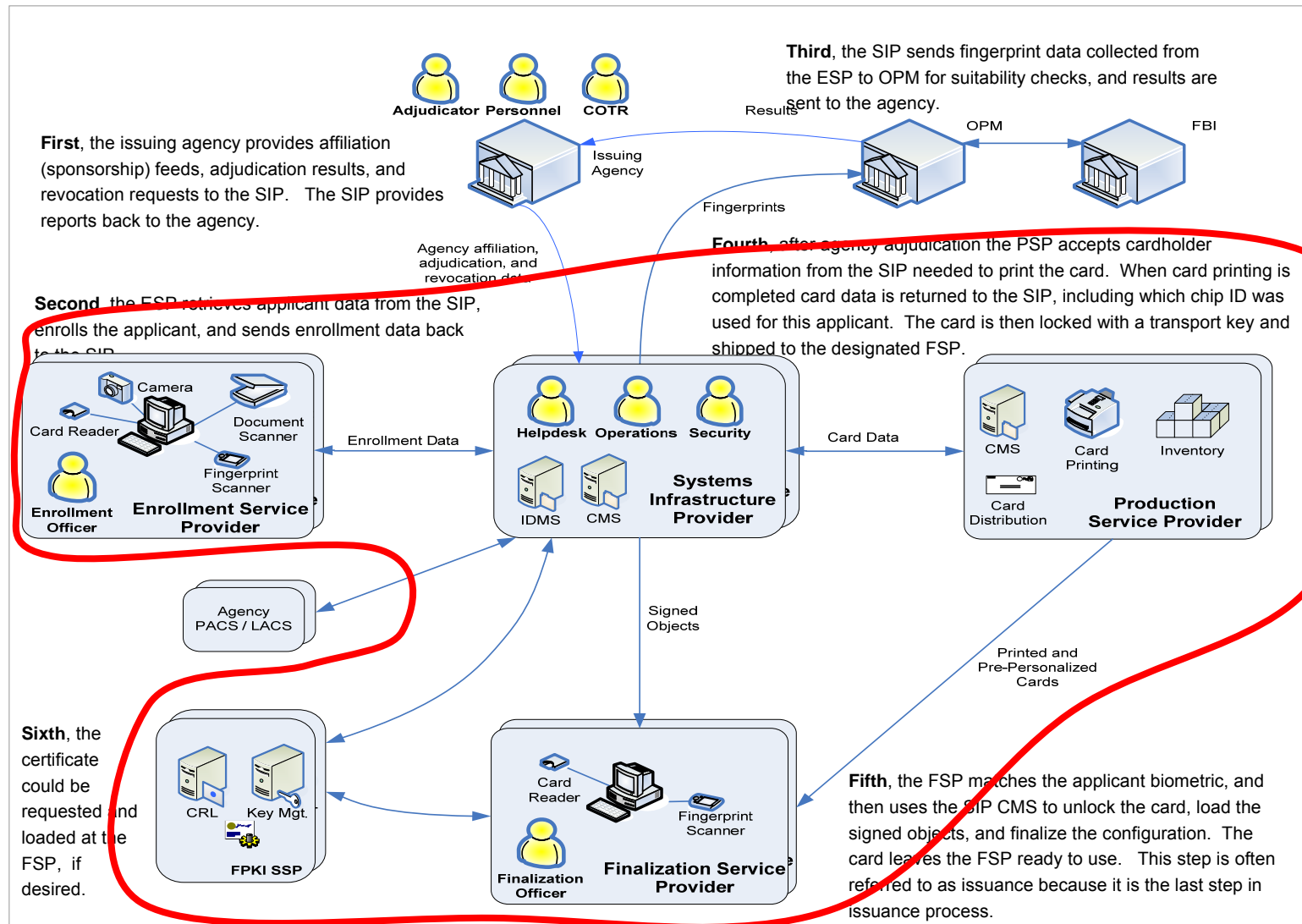**Security Industry Association/Smart Card Alliance**
August 23, 2006

Key Milestones

Timeline	Agency/Department Requirement/Milestone
☑ **August 27, 2004**	HSPD-12 signed and issued
☑ Not later than 6 months (**February 27, 2005**)	NIST Issue standard (FIPS-201)
☑ Not later than 8 months following issuance of standard (**October 27, 2005**)	Compliance with FIPS-201 Part One: Identity Proofing and Enrollment. **PIV-I**
Not later 20 months following issuance of standard (**October 27, 2006**)	Commence deployment of FIPS-201 compliant Identity Credentials (FIPS-201 Part Two). **PIV-II**
Not later than 32 months following issuance of standard (**October 27, 2007**)	Compliance with FIPS-201 Part Two: Fully operational Physical and Logical Access

E·GOV

Where are we today?
65 days -- counting weekends

- 9 agencies committed to their own infrastructure
  - ✓ DHS, DoD, NASA, DoS, SSA, EPA, NSF, HHS, Treasury
  - ✓ Several RFPs on the street

- 100+ Agencies want to share infrastructure
  - ✓ All small agencies
  - ✓ ED, HUD, USDA, DOI, GSA committed
  - ✓ Several undecided

- Shared Service Providers
  - ✓ 8 serviced by DoS
  - ✓ DOI RFP issued July 24 for agencies serviced by DOI HR
  - ✓ GSA shared service award

- GSA Government-wide Shared Service
  - ✓ Award 8/18/06
  - ✓ Intended for government-wide use
  - ✓ Agencies to sign MOU and Interagency Agreement by September 30
  - ✓ GSA MSO established, Mike Butler assigned on detail

HSPD-12 Shared Services Architecture

Third, the SIP sends fingerprint data collected from the ESP to OPM for suitability checks, and results are sent to the agency.

**First**, the issuing agency provides affiliation (sponsorship) feeds, adjudication results, and revocation requests to the SIP.   The SIP provides reports back to the agency.

Fourth, after agency adjudication the PSP accepts cardholder information from the SIP needed to print the card. When card printing is completed card data is returned to the SIP, including which chip ID was used for this applicant. The card is then locked with a transport key and shipped to the designated FSP.

Second, the ESP retrieves applicant data from the SIP, enrolls the applicant, and sends enrollment data back to the SIP.

Adjudicator Personnel COTR

Results

OPM

FBI

Issuing Agency

Fingerprints

Agency affiliation, adjudication, and revocation data

Camera

Card Reader

Document Scanner

Fingerprint Scanner

Enrollment Officer

Enrollment Service Provider

Enrollment Data

Helpdesk Operations Security

IDMS CMS

Systems Infrastructure Provider

Card Data

CMS

Card Printing

Inventory

Card Distribution

Production Service Provider

Agency PACS / LACS

Signed Objects

Printed and Pre-Personalized Cards

Sixth, the certificate could be requested and loaded at the FSP, if desired.

CRL

Key Mgt.

FPKI SSP

Card Reader

Fingerprint Scanner

Finalization Officer

Finalization Service Provider

Fifth, the FSP matches the applicant biometric, and then uses the SIP CMS to unlock the card, load the signed objects, and finalize the configuration. The card leaves the FSP ready to use.   This step is often referred to as issuance because it is the last step in issuance process.

HSPD-12 Federal Shared Enrollment Service

Station 1
Station 2
Station 3
Station 4
Station 5
Station 6
Station 7
Station 8
Station "n"

Add. Needs Stations

Enrollment Broker

Dual Site Shared Centralized Components

- **Card Mgmt System**
- **ID Mgmt System**
- **Card Printing System**
- **PKI Certificate Integration**

Other HSPD-12 Centralized Answers
(a authorized by OMB)

• up to 450+ geographically distributed & shared enrollment stations;
• GSA/other agencies provide leased space, operators

GSA

E·GOV

Sharing Opportunities

- Enrollment Stations – largest single cost; largest opportunity for savings

- Centralized Components – "fixed cost" item whether 10,000 card holders or 1 million card holders

- Interfaces – why build interfaces from OPM, FBI, etc more than once? Even with std. specs, there are significant costs for each "build"
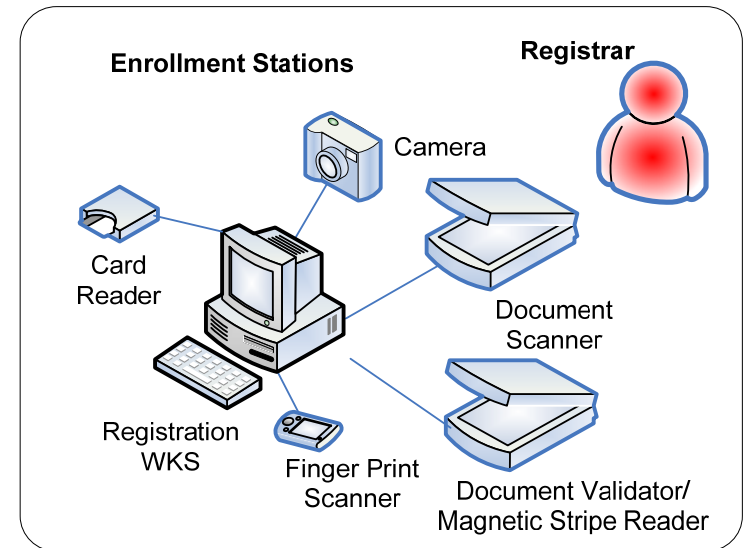
- Other Opportunities - TBD

E·GOV
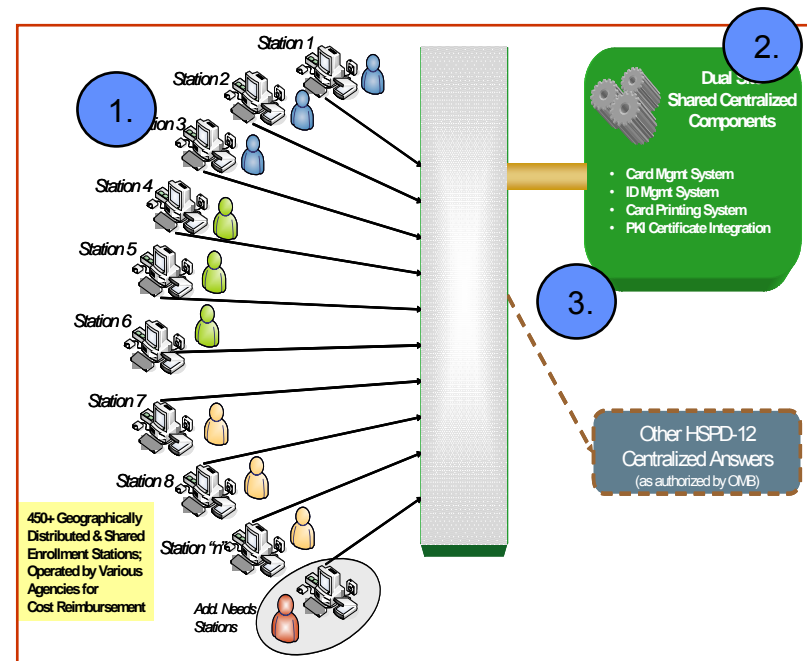
GSA Shared Infrastructure for HSPD-12 Enrollment Station Rollout
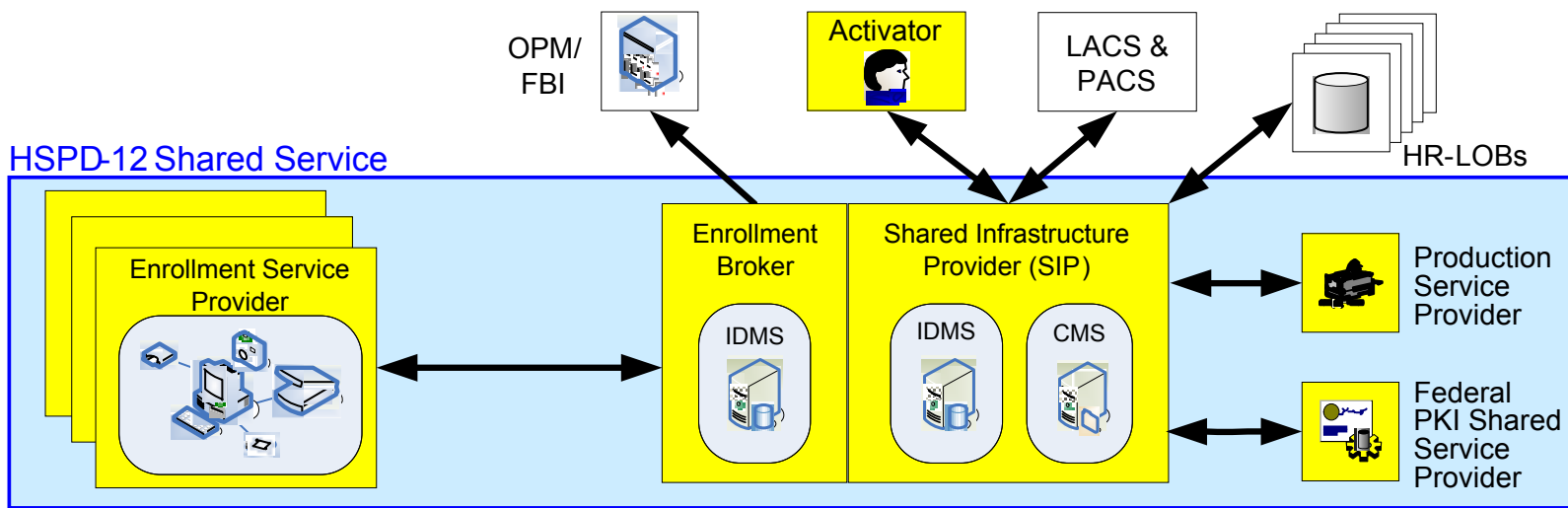
- *Phases for Enrollment/Issuance Station Rollout :*

- **Phase 1 → 80% of Shared Service Workforce**
    - Stations in 120 Key Metropolitan Areas located so that Federal Workforce travels maximum of 25 Miles to Enrollment from Duty Station
- **Phase 2 → 90+% of Shared Workforce**
    - Fixed and mobile stations in additional Key Areas
- **Phase 3 → On-going Operations & Maintenance**

An Enrollment Station is a location where the Federal Workforce can provide identity information to the Certified Registrar for processing.
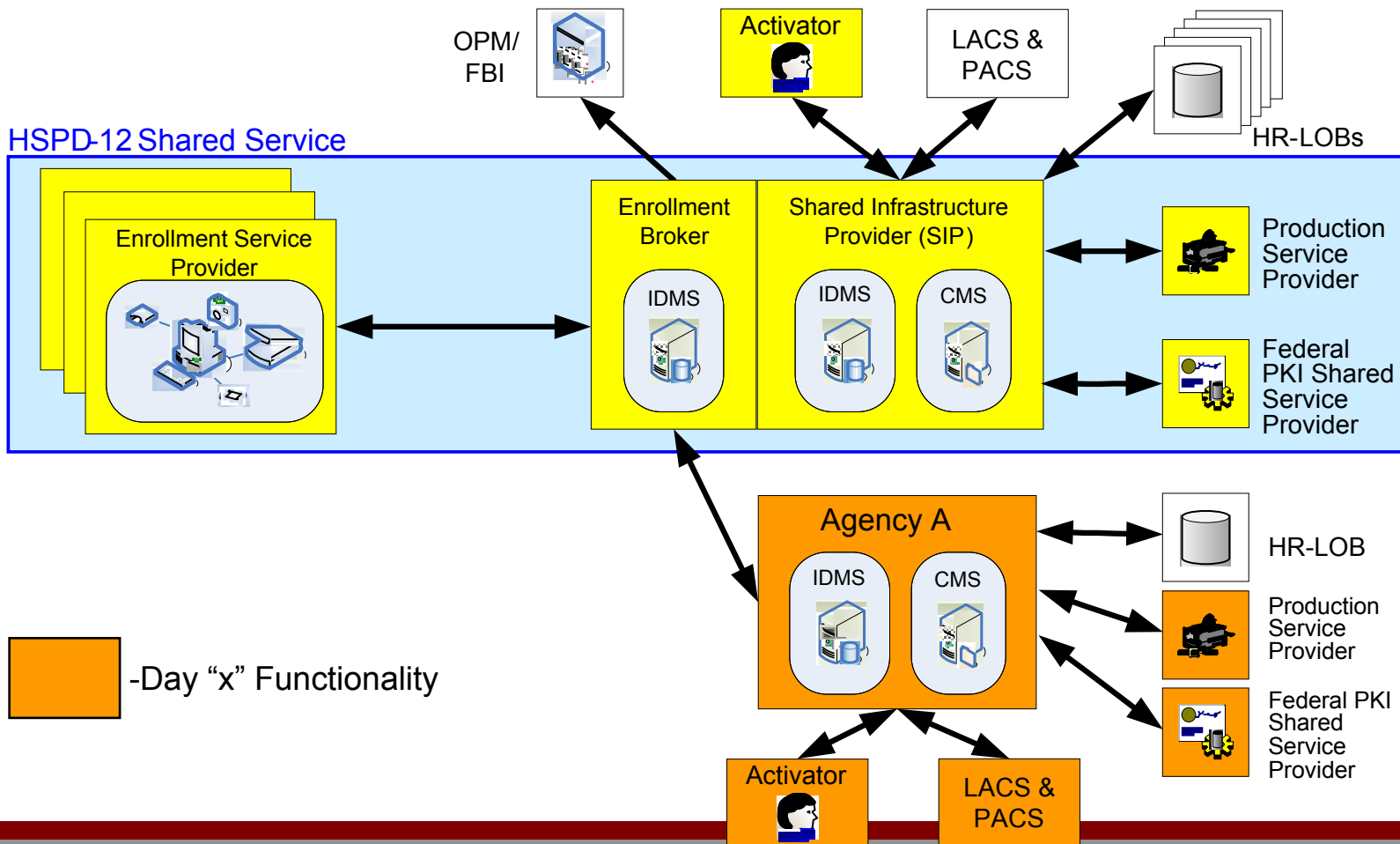

Enrollment Stations — Registrar — Camera — Card Reader — Document Scanner — Registration WKS — Finger Print Scanner — Document Validator/ Magnetic Stripe Reader

Standard PIV data feed

E·GOV

HSPD-12 Shared Services – Initial Operating Capability

- Day 1 Functionality

HSPD-12 Shared Services – Enhanced Operating Capability

HSPD-12 Shared Service

OPM/ FBI

Activator

LACS & PACS

HR-LOBs

Enrollment Service Provider

Enrollment Broker
IDMS

Shared Infrastructure Provider (SIP)
IDMS   CMS

Production Service Provider

Federal PKI Shared Service Provider

-Day "x" Functionality

Agency A
IDMS   CMS

HR-LOB

Production Service Provider

Federal PKI Shared Service Provider

Activator

LACS & PACS

HSPD-12 Shared Services – Enhanced Operating Capability

FAR Amendments for Implementation of HSPD-12
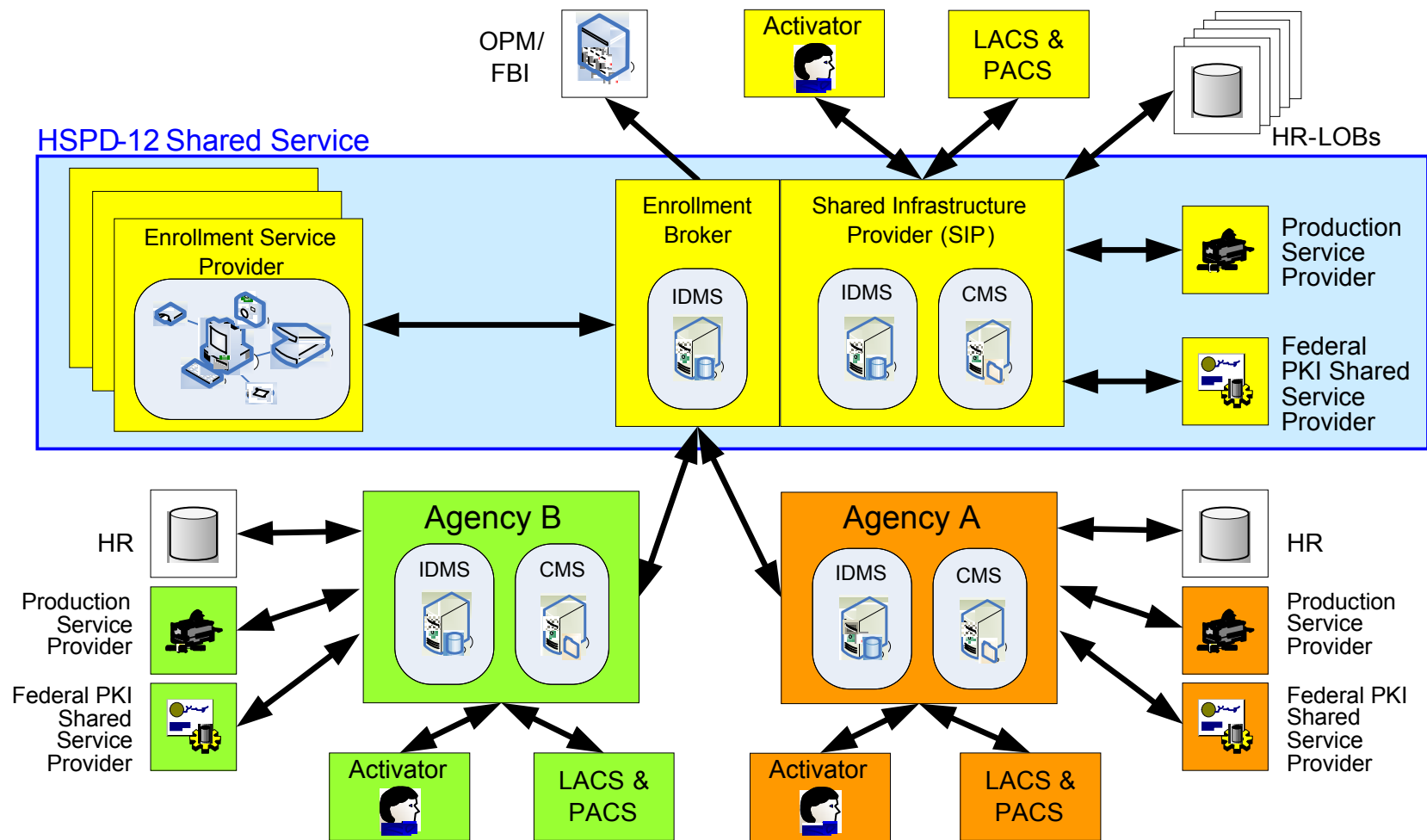
- FAR Interim Rule: Common Identification Standard for Contractors

  ✓ Published January 3, 2006; applies to solicitations/contracts issued on/after October 27, 2005

  ✓ Contractors must comply with PIV requirements for personnel needing routine access to Federal facilities and/or information systems

  ✓ Coordinated and issued by Civilian Acquisition Council (CAC) and Defense Acquisition Regulations (DAR) Council.

- FAR Case 2005-017: Requirement to Purchase Approved Authentication Products and Services

  ✓ To be issued as Proposed Rule, 8/23.

  ✓ Requires agencies to use only FIPS 201 approved products and services for the implementation of HSPD-12.

Conclusion

We are where we are today…..

It ain't pretty …..

Lots and lots of moving parts…

Gotta move forward …

I believe we'll achieve the goal.

For More Information

- Visit our Websites:

  http://www.idmanagement.gov

  http://www.cio.gov/ficc

  http://www.cio.gov/fpkipa

  http://www.csrc.nist.gov/piv-project

- Or contact:

  David Temoshok

  Director, Identity Policy and Management

  202-208-7655

  david.temoshok@gsa.gov

E·GOV